CLAIMS

We claim:

1. A system to enforce privacy preferences on exchanges of personal data comprising of one or more computers connected to one or more networks through one or more network interfaces, each computer having one or more memories and one or more central processing units (CPUs), the system further comprising:

one or more data-subject rule sets that has one or more subject constraints on one or more private, subject data releases;

a receiving process that receives a request message from a data-requester over the network interfaces, the request message having one or more requests for one or more of the private, subject data releases pertaining to a subject, and a requester privacy statement for each of the respective private data; and

a release process that compares the requester privacy statement to the subject constraints and releases the private, subject data release in a response message to the requester only if the subject constraints are satisfied.

2. A system, as in claim 1, where the requester also has to be authorized to receive the private data.

3. A system, as in claim 2, where there is more than one level of authorization.

4. A system, as in claim 1, wherein each of the subject constraints further comprises:

an authorization dataset describing the data to which the constraint applies;

a privacy preference rule that describes the privacy preferences under which the data may be released and the corresponding actions allowed;

an access list describing who is allowed to access the data; and

an authorization action that describes any additional action to be taken if the restrictions imposed by the authorization dataset, the privacy preference rule and the access list of this constraint are matched.

5. A system, as in claim 1, wherein the private, subject data release further comprises:

one or more subject data that is owned and held by the data-subject;

one or more subject data that is owned by the data-subject, but held by one or more parties on behalf of the data subject; and

one or more subject data that is owned and held by one or more third parties.

6. A system, as in claim 1, where one or more of the requesters have to satisfy different subject rule sets for the same private data.

7. A system, as in claim 1, where the private, subject data release is partitioned into a first part that satisfies the constraints and is released and a second part that does not satisfy the constraints and is not released.

8. A system, as in claim 1, wherein the private, subject data released further comprises one or more data for which additional manual authorization from the subject is needed before the data is released.

9. A system, as in claim 1, wherein the private, subject data released further comprises one or more missing values which have to be acquired from the subject before the data is released.

10. A system, as in claim 1, wherein private, subject data released further comprises one or more data that is stored with one or more third parties and has to be retrieved from the third parties before the private, subject data release can be released.

11. A system, as in claim 1, wherein the private, subject data released further comprises one or more data that is stored with one or more third parties and the third parties have to be provided with authorization to release the data to the requester.

12. A system, as in claim 1, where the private, subject data release to which each constraint applies comprises one or more of the following: one or more classes of data, one or more properties of data, and one or more instances of data.

13. A system, as in claim 1, where the private, subject data release is ordered in a hierarchy with one or more levels and each of the levels has one or more constraints that apply to the respective private, subject data release in the level.

14. A system, as in claim 13, where one or more of the levels have different constraints.

15. A system, as in claim 13, where one or more of the levels inherits one or more of the constraints from one or more other levels.

16. A system, as in claim 13, where the level to which each constraint applies further comprises one or more of the following: one or more classes of data, one or more properties of data, and one or more instances of data.

17. A system, as in claim 1, where the constraints include privacy preferences based on any one or more of the Platform for Privacy Preferences (P3P) standard privacy statements, including a purpose, a retention, a recipient and an access.

18. A system, as in claim 1, where the data includes any one or more of the following: a privacy data, a privacy data associated with a natural person, a confidential information, and a trade secret.

19. A method to enforce privacy preferences on exchanges of personal data, comprising the steps of:

specifying one or more data-subject rule sets, the data-subject rule set having one or more subject constraints on one or more private, subject data releases;

receiving a request message from a data-requester, the request message having one or more requests for one or more of the data releases pertaining to the subject, and a requester privacy statement for each of the respective private, subject data release;

comparing the requester privacy declaration to the subject constraints; and

releasing the private, subject data release in a response message to the requester only if the subject constraints are satisfied.

20. The method of claim 19, further comprising the step of authorizing the requester to receive the private, subject data release.

21. The method of claim 20, wherein the step of authorizing the requester includes the steps of authorization at more than one level.

22. The method of claim 19, wherein the step of specifying each of the subject constraints includes the steps of:

specifying an authorization dataset describing the data to which the constraint applies;

specifying a privacy preference rule that describes the privacy preferences under which the private, subject data release may be released and the corresponding actions allowed;

specifying an access list describing who is allowed to access the said data; and

specifying an authorization action that describes any additional action to be taken if the restrictions imposed by the authorization dataset, the privacy preference rule and the access list of this constraint are matched.

23. The method of claim 19, wherein the step of specifying each of the subject constraints includes the steps of:

specifying such constraints for subject data that owned and held by the subject;

specifying such constraints for private, subject data that is owned by the data subject, but held by one or more parties on behalf of the subject; and

specifying such constraints for private subject data that is owned and held by one or more third parties.

24. The method of claim 19, wherein the step of specifying each said subject rule sets includes the steps of specifying different subject rule sets for the same private data for one or more requesters that must be satisfied for them to get the private, subject data release.

25. The method of claim 19, wherein the step of comparing the requester privacy declaration to the subject constraints includes the step of partitioning the private data into a first part that satisfies the constraints and is released and a second part that does not satisfy the constraints and is not released.

26. The method of claim 19, wherein the step of releasing the data includes the step of getting manual authorization from subject for some of the data before releasing the data.

27. The method of claim 19, wherein the step of releasing the data includes the step of getting one or more missing values from subject before releasing the data.

28. The method of claim 19, wherein the step of releasing the data includes the step of getting one or more subject data from one or more third parties, that store that subject data, before releasing the data.

29. The method of claim 19, wherein the step of releasing the data includes the step of providing authorization to one or more third parties holding part of the private, subject data release to release the part to the requester.

30. The method of claim 19, wherein the step of specifying each of the subject constraints includes the steps of:

ordering the data in a hierarchy with one or more levels; and

specifying one or more constraints for each level that apply to the data in that level.

31. The method of claim 19, wherein the step of specifying each said subject constraint includes the step of specifying one or more of the following: one or more classes of data, one or more properties of data, and one or more instances of data..

32. The method of claim 30, wherein the step of specifying constraints for each level includes the step of specifying different constraints for one or more of the levels.

33. The method of claim 30, wherein the step of specifying constraints for each level includes the step of inheriting the constraints from one or more other levels.

34. The method of claim 30, wherein the step of ordering the data into a hierarchy of levels includes the step of creating levels from one or more classes of data, properties of data, instances of data, or a combination of these.

35. The method of claim 19, wherein the step of specifying each said subject constraint includes the steps of specifying constraints that include privacy preferences based on any one or more of a Platform for Privacy Preferences (P3P) standard privacy statements.

36. A method, as in claim 35 where the standard privacy statements include any one or more of the following: a purpose, a retention, a recipient and an access.

37. The method of claim 19, wherein the step of specifying each said subject constraint includes the steps of specifying constraints over subject data that includes any one or more of the following: a privacy data, a privacy data associated a natural person, a confidential information, and a trade secret.

38. A system of doing business of enforcing privacy preferences on exchanges of personal data comprising :

a trusted third-party acting as a personal-data-service (PDS) on behalf of a data-subject and providing one or more computers connected to one or more networks through one or more network interfaces, each computer having one or more memories and one or more central processing units, to host subject data and policies, receive and process requests for such data and release as well as authorize release of such data; and

one or more third-parties holding additional data about the data-subject on one or more computers connected to one or more networks through one or more network interfaces, each computer having one or more memories and one or more central processing units,

the system further comprising:

one or more data-subject (subject) rule sets hosted by the PDS that has one or more subject constraints on one or more private, subject data releases, such data being hosted by the PDS or one or more said third-parties;

a receiving process executed by the PDS that receives a request message from a data-requester (requester) over the network interfaces, the request message having one or more requests for one or more of the data releases pertaining to the subject, and a requester privacy statement for each of the respective private data; and

a release process executed by the PDS that compares the requester privacy declaration to the subject constraints (authorization rules) and, if the subject constraints are satisfied, gathers, releases and authorizes release of such data, whether hosted by the PDS or one or more third parties, in a response message to the requester.

39. A system of doing business, as in claim 38, where some of the said subject data and policies are held on, and released by, one or more of the data subject's own computers that are also connected to one or more networks through one or more network interfaces, each computer having one or more memories and one or more central processing units.

40. A method of doing business of enforcing privacy preferences on exchanges of personal data, the method comprising the steps of:

selecting and using a trusted third-party to act as a personal-data-service (PDS) on behalf of a data-subject;

specifying data profiles containing private subject data, that is owned by the data subject, with the PDS;

specifying one or more data-subject rule sets with the PDS that has one or more subject constraints on one or more private, subject data releases, such data being hosted by the PDS or one or more third-parties;

receiving of a request message, by the PDS, from a data-requester (requester), the request message having one or more requests for one or more of the data releases pertaining to the subject, and a requester privacy statement for each of the respective private data;

comparing, by the PDS, the requester privacy declaration to the subject constraints;

gathering and releasing the data from the data stored with the PDS as well as data owned and stored with one or more third parties, as well as authorizing release of such data held by one or more third parties, in a response message to the requester only if the subject constraints are satisfied.

41. A method of doing business, as in claim 40, further including the steps of setting up some of the private subject data and constraints on personal systems of the data subject, and providing such data and constraints upon request to the PDS.

42. A system of doing business of enforcing privacy preferences on exchanges of personal data comprising one or more third-parties owning and holding data about the data-subject on one or more computers connected to one or more networks through one or more network interfaces, each computer having one or more memories and one or more central processing units, the system further comprising:

one or more data-subject rule sets hosted by each such third-party that has one or more subject constraints on one or more private, subject data releases, such data being hosted by each of the said third-parties;

a receiving process executed by each of the said third-parties that receives a request message from a data-requester over the network interfaces, the request message having one or more requests for one or more of the data releases pertaining to the subject held by said third parties, and a requester privacy statement for each of the respective private data; and

a release process executed by the each of the said third-parties that compares the requester privacy declaration to the subject constraints (authorization rules) and, if the subject constraints are satisfied, gathers and releases such data in a response message to the requester.

43. A system as in claim 42, where a trusted third-party acting as a personal-data-service (PDS) on behalf of a data-subject and providing one or more computers connected to one or more networks through one or more network interfaces, each computer having one or more memories and one or more central processing units, to host data owned by a data subject, policies of such data subject, receive and process requests for such data and release such data

44. A system, as in claim 43, where some of the subject data and policies are held on, and released by, one or more of the data subject's own computers that are also connected to one or more networks through one or more network interfaces, each computer having one or more memories and one or more central processing units.

45. A method of doing business of enforcing privacy preferences on exchanges of personal data, said method comprising the steps of:

specifying one or more data-subject rule sets that has one or more subject constraints on one or more private, subject data releases, such subject data being owned and hosted by one or more third-parties;

receiving of a request message, by any of the third-parties, from a data-requester (requester), the request message having one or more requests for one or more of the data releases pertaining to the subject that is held by said third-party, and a requester privacy statement for each of the respective private data;

comparing, by said third-party receiving the request, the requester privacy declaration to the subject constraints; and

releasing the data, from the subject-data owned and stored by said third-party receiving the data request, in a response message to the requester only if the subject constraints are satisfied.

46. A method of doing business, as in claim 45, including the steps of:

selecting and using a trusted third-party to act as a personal-data-service (PDS) on behalf of a data-subject;

specifying data profiles containing private subject data, that is owned by the data subject, with the PDS;

specifying one or more data-subject (subject) rule sets with the PDS that has one or more subject constraints on one or more private, subject data releases, such data being hosted by the PDS;

receiving of a request message, by the PDS, from a data-requester (requester), the request message having one or more requests for one or more of the data releases pertaining to the subject and held by the PDS, and a requester privacy statement for each of the respective private data;

comparing, by the PDS, the requester privacy declaration to the subject constraints; and

releasing the data from the data stored with the PDS in a response message to the requester only if the subject constraints are satisfied.

47. A method of doing business, as in claim 46, including the steps of setting up some of the private subject data and constraints on personal systems of the data subject, and providing such data and constraints upon request to the PDS.